RENTABILIDAD DE LAS MEDIDAS DE SEGURIDAD

LINDK: http://www.seguridaddelainformacion.com/seg_10.htm

Dentro del sector de la seguridad de la información se reconoce tanto la necesidad de evaluar el Retorno de la Inversión en Seguridad, como la dificultad de realizar cálculos cuantitativos que lo reflejen.

En adelante nos referiremos a la seguridad de la información simplemente como “seguridad”.

La necesidad de invertir en medidas de seguridad surge principalmente para evitar el coste que suponen los incidentes, sean estos ataques, errores o accidentes. El coste directo de un incidente puede ser la pérdida de ingresos (lucro cesante en términos legales), los daños y pérdidas tanto de propiedad como pérdidas económicas directas. A esto hay que sumarle el coste de devolver el sistema al estado anterior al incidente. Para determinados incidentes puede haber otros costes directos como vidas humanas, pérdida de información o multas.

Entre los costes indirectos de los incidentes podemos citar la pérdida de imagen, la pérdida de la confianza de clientes y accionistas, problemas inducidos en el flujo de caja, el incumplimiento de contratos y otras responsabilidades legales; el incumplimiento de obligaciones sociales o morales y otros costes adicionales.

Las medidas de seguridad en que se invierte para evitar estos costes son sólo una parte de la historia de la seguridad de un sistema a lo largo de su ciclo de vida. Con demasiada frecuencia la seguridad no se considera en los estados iniciales del desarrollo de un sistema de información, lo que lleva a utilizar medidas de seguridad que parchean defectos en su diseño e implementación. Veamos algunas medidas aconsejables en las fases del ciclo de vida de un sistema:

1. Fase de Toma de Requerimientos: Además de los requerimientos de negocio, del usuario, y técnicos, es conveniente y suele ser rentable considerar requerimientos de seguridad, como control de accesos, secreto, trazas y disponibilidad.
2. Fases de Análisis y Diseño: Los requerimientos de control de accesos, secreto, trazas y disponibilidad pueden traducirse en un sistema potencialmente seguro, que incluso puede no requerir medidas de seguridad adicionales.
3. Fase de Construcción; Durante esta fase debe evitarse utilizar características de la tecnología utilizada que puedan introducir debilidades en el sistema.

4. Fase de Control de Calidad: En este caso se simulan usuarios autorizados en el sistema, que prueban los requerimientos de negocio, de usuario, técnicos y de seguridad. Los posibles fallos de seguridad suelen manifestarse como comportamientos inesperados del sistema (debilidades), que no están en los requerimientos. Para descubrir estos comportamientos se simulan usuarios que intentar realizan operaciones no autorizadas o romper el sistema.
5. Fase de Implementación o puesta en producción: Durante esta fase hay que evitar la modificación no autorizada del software que se ha probado, garantizando que se implanta el mismo software que se ha probado.

Medida de la Rentabilidad
¿Qué sabemos intuitivamente acerca del riesgo y el coste de las medidas de seguridad? Realmente existe una relación compleja entre los factores que afectan al riesgo, como la ventana de oportunidad, el valor del activo y su valor para el atacante, el parque de activos, el número de incidentes, el coste de estos, etc. También sabemos que cuando ponemos medidas para paliar el riesgo las facilidades de uso y gestión de los sistemas disminuirán, lo que supone un coste indirecto de las medidas de seguridad.

La figura siguiente indica cualitativamente la relación entre todos estos factores. Las flechas indican los factores que afectan directamente al coste de la amenaza, apreciándose además que la inversión en medidas de seguridad (Coste de la Medida) disminuye el coste de la amenaza.

¿Cómo pasar de esta intuición a información cuantitativa? Hay cierto conocimiento acumulado acerca de la relación entre la inversión en medidas de seguridad y sus resultados. Tenemos la paradoja de Mayfield, que demuestra que tanto dar acceso universal a un sistema como restringir absolutamente este acceso tiene un coste infinito, mientras que los casos intermedios tienen un coste aceptable.

También tenemos un estudio empírico del CERT de la Universidad Carnegie Mellon que afirma que cuanto más gastas en medidas de seguridad, menos diferencia supone en la misma. Esto quiere decir que una vez realizada una inversión razonable en las medidas de seguridad no por gastar el doble vamos a estar el doble de seguros.

El estudio más fácil de encontrar sobre este tema en Internet cita las fórmulas ideadas durante la implantación de un sistema de detección de intrusiones por un equipo de la Universidad de Idaho.

R: pérdidas.
E: pérdidas evitadas.

T: coste total de las medidas de seguridad.

(R-E)+ T = ALE

R-ALE = ROSI, luego ROSI = E-T

Lo malo de esta fórmula es que E es una pura estimación, y más aún si la medida que se trata en un IDS, que simplemente recoge información sobre intrusiones, por lo que no hay una relación causa efecto entre detectar una intrusión y evitar un incidente. Mezclar este tipo de estimaciones sin base alguna con fórmulas matemáticas es como mezclar magia con física.

¿Con qué problemas nos enfrentamos para calcular el retorno de inversión de las medidas de seguridad? El más importante es la falta de datos reales, no muy lejos de la serie de suposiciones y medias verdades comúnmente aceptadas, como que el riesgo disminuye según aumenta la inversión y que el retorno de la inversión es positivo para todos los niveles de inversión.

Nadie invierte en medidas de seguridad para ganar dinero. Se invierte porque no queda más remedio. El retorno de inversión sirve para demostrar que invertir en seguridad es beneficioso, para seleccionar las mejores medidas de seguridad con un presupuesto dado, y para determinar si el presupuesto dedicado a seguridad es suficiente para cumplir con los objetivos de negocio, pero no para mostrar que se gane dinero con esta inversión.

Tanto de forma general como desde el punto de vista del retorno de inversión hay dos tipos de medidas de seguridad, las medidas que reducen la vulnerabilidad y las que reducen el impacto.

• Las medidas que reducen la vulnerabilidad apenas reducen el impacto en caso de producirse un incidente. Estas medidas protegen de un rango estrecho de amenazas. Se conocen normalmente como medidas Preventivas. Como ejemplos de estas medidas tenemos los cortafuegos, los candados y las medidas de control de accesos. Un ejemplo de la estrechez del rango de protección es el uso de cortafuegos que protege contra el acceso a direcciones y puertos no autorizados, pero no contra la difusión de gusanos ni contra el spam.

• Las medidas que reducen el impacto apenas reducen la vulnerabilidad en caso de producirse un incidente. Estas medidas protegen de un amplio espectro de amenazas. Se conocen habitualmente como medidas Paliativas. Como ejemplos de estas medidas tenemos los discos RAID, las copias de seguridad y los enlaces de comunicación redundantes. Un ejemplo de la amplitud del rango de protección es el uso de copias de seguridad, que no evitan incidentes, pero protegen de pérdidas de información efectivas ante fallos físico y lógicos de todo tipo.

La rentabilidad de ambos tipos de medidas son diferentes, como veremos a continuación.

Medidas de Reducción de Vulnerabilidad o Preventivas

Una reducción de vulnerabilidad se traduce en una reducción del número de incidentes. Por tanto las medidas de seguridad que reducen la vulnerabilidad son rentables cuando previenen incidentes por un valor superior al coste total de la medida en ese periodo de inversión.

Puede utilizarse para el cálculo la siguiente fórmula:

ROSI = (CAantes – CAdespues) / MScoste

CA = Coste del Amenaza = Número de Incidentes * Coste de un Incidente.

Cuando ROSI > 1, la medida de seguridad es rentable.

Calcular el coste de la amenaza como número de incidentes multiplicado por el coste de cada incidente es una alternativa respecto del cálculo tradicional de probabilidad del incidente multiplicado por el coste del incidente, siempre que el número de incidentes en el periodo de inversión sea superior a 1. Para calcular matemáticamente una probabilidad es necesario conocer el número de casos favorables y el número de casos posibles. Es rara la organización que dispone de información sobre los casos posibles (pero no “favorables”) de incidentes. Faltando esta información, no es posible calcular la probabilidad. Sin embargo, es relativamente sencillo conocer los incidentes producidos en un plazo de tiempo y su coste.

Para que una probabilidad conocida tenga capacidad predictiva, es necesario además disponer de una cantidad suficientemente grande de casos y que las condiciones no cambien. Si tenemos en cuenta la complejidad de comportamiento de los atacantes y de las organizaciones que utilizan sistemas de información, es aventurado suponer las condiciones como constantes. Por consiguiente, calcular el coste de una amenaza mediante información probabilística se revela como poco fiable en condiciones reales.

Una ventaja importante de calcular el coste de una amenaza como CA = N Incidentes * C Incidente es que integra en una sola fórmula el coste de los incidentes, la probabilidad y el parque de activos, dado que el número de incidentes depende en parte del tamaño del parque. Para hacer un cálculo de rentabilidad como este necesitamos información real sobre los incidentes y su coste, información que hay que recolectar, lo que supone un coste indirecto de la gestión de la seguridad en la organización.

La rentabilidad de una medida de reducción de vulnerabilidad

depende del entorno. Por ejemplo en un entorno en el que se producen muchos incidentes, la medida de seguridad será más rentable que en otro donde no se producen. Mientras que usar un cortafuegos personal en PC conectado a Internet las veinticuatro horas puede ser rentable, hacerlo en una red privada no conectada a Internet, no lo será. Invertir en una puerta blindada en muchas regiones de España es rentable, mientras que ciertas áreas rurales de Canadá, es tirar el dinero.

Ejemplo de cálculo de rentabilidad:

1. Hay dos hurtos de un parque de 50 portátiles en un año.
2. Reemplazar un portátil cuesta 1800 euros.
3. Al año siguiente hay 75 portátiles en la compañía.
4. Se protegen los portátiles con candados de 60€.
5. Al año siguiente sólo hay un hurto de portátil.

ROSI = (R antes – R despues) / MS coste

ROSI = ((1800 + Vi)*3 - ((1800+ Vi)*1+75*60))/(75*60)

(El número de incidentes esta ajustado para el incremento del número de objetivos).

Si la información de un portátil no valiera nada (Vi=0), la medida de seguridad no salen rentable (ROSI < 1). En este ejemplo, los candados de 60€ son rentables cuando la información de un portátil vale más de 2700€, o cuando basándonos en información histórica, podemos esperar 5 hurtos este año.

Con este tipo de análisis, podríamos:

• Usar candados sólo para los portátiles con información valiosa.
• Calcular el precio máximo de candados para todos los portátiles (24€ cuando Iv=0).

Medidas de Reducción de Impacto o Paliativas

Dado que las medidas de reducción de impacto no evitan incidentes, el cálculo anterior no es aplicable. En el mejor caso estas medidas no se usan nunca, mientras que cuando hay dos incidentes que podrían suponer la destrucción de los activos protegidos, parecen valer el doble que estos activos.. Ahora bien ¿quien gastaría el doble del valor de un activo en medidas de seguridad? No se puede medir la rentabilidad de las medidas de reducción de impacto. Estas medidas son como los seguros, ponen un límite a la máxima pérdida sufrida en caso de un incidente.

Lo importante de las medidas de reducción de impacto es qué protección obtienes por tu dinero. La eficacia de esta protección si se puede medir, como por ejemplo según el tiempo de recuperación después de un incidente. Según su eficacia hay

medidas desde las copias de seguridad (con cierto coste extra) hasta sistemas totalmente redundantes (con coste por encima del doble).

Presupuesto, coste y selección de medidas
El presupuesto de seguridad debería ser como máximo igual a las pérdidas esperadas debidas a ataques, errores y accidentes en los sistemas de información para el año contable. En caso contrario, quedaría garantizada su falta de rentabilidad. En el siguiente gráfico se representan las pérdidas esperadas por el área subyacente a la curva. Por claridad del gráfico este representa el de una empresa con unas pérdidas esperadas enormes, de casi el 25% del valor de la compañía. En empresas reales este gráfico puede ser más legible usando escalas logarítmicas.

Al evaluar el coste de una medida de seguridad se deben considerar tanto sus costes directos de hardware, software e implantación como sus costes indirectos, entre los que se pueden encontrar su control de calidad mediante evaluación de incidentes, el hacking ético (simulación de ataques), auditorias, simulación de incidentes, análisis forenses y auditorias de código.

Es frecuente ver como las medidas de seguridad se seleccionan basándose en el miedo, la incertidumbre y la duda, o bien en la paranoia, en el seguimiento de la moda, o simplemente en el azar. Sin embargo el cálculo de la rentabilidad de medidas de seguridad puede ayudar a seleccionar las mejores medidas con un presupuesto dado. Parte del presupuesto puede dedicarse a la protección de activos críticos mediante medidas de reducción de impacto, y otra parte a la protección del conjunto de todos los activos mediante medidas de reducción de la vulnerabilidad.

Conclusiones
Las conclusiones más importantes a extraer de todo lo dicho, son las siguientes:

• Para garantizar la máxima eficiencia de nuestra inversión es necesario, y posible si tenemos datos en que apoyarnos, calcular el retorno de la inversión de las medidas de reducción de Vulnerabilidad.
• Para poder hacer cálculos reales necesitamos información real sobre el coste de los incidentes en nuestra empresa o en empresas comparables del mismo sector.
• Tanto los incidentes como las medidas de seguridad tienen componentes de coste directos e indirectos, que hay que considerar al hacer cálculos de rentabilidad.
• Tomar en cuenta los requerimientos de seguridad desde el principio del ciclo de vida de los sistemas de información supone un ahorro a largo plazo, dado que necesitaremos menos medidas de seguridad, o medidas menos sofisticadas.
• Las medidas de reducción de impacto se deben seleccionar en función de su eficacia y del presupuesto de que dispongamos, dado

que el cálculo de su rentabilidad no es práctico, igual que no se puede calcular la rentabilidad de un seguro.

Vicente Aceituno Canal

Autor de “Seguridad de la Información”

Referencias

• University of New Haven "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security"
• Carnegie Mellon University “The Survivability of Network Systems: An Empirical Analysis”
• CIO Magazine "Finally, a Real Return on Security Spending"